

Stichworte: Elliptische Kurven über endlichen Körpern, $N_p = \#E(\mathbb{F}_p)$, Defekt, Satz von Hasse, Birch & Swinnerton-Dyer-Vermutung, komplexe Multiplikation (CM), gute/schlechte Reduktion, Spur des Frobenius, Text in elliptische Kurve einbetten

§3.3 Elliptische Kurven über \mathbb{F}_p und \mathbb{F}_{p^r}

- 1.) Elliptische Kurven über endlichen Körpern werden vielfältig eingesetzt, zum einen in der Kryptographie, zum anderen auch in technischen Systemen mit wenigen Ressourcen (eingebettete Systeme), z.B. Steuergeräte in Automobilen (elektronische Wegfahrsperren, Tuning-Schutz, Car-to-Car-Kommunikation, etc.). Manche Hardware-Implementierungen arbeiten über \mathbb{F}_2^r der Charakteristik 2, bei denen die technische Umsetzung damit günstig ist.

3.3.1 Punkte zählen, der Frobenius

- 2.) Wir studieren zunächst elliptische Kurven über \mathbb{F}_p , wo p prim, mit der "modularen Brille" mod p . Das Verhalten dieser Kurven kann ganz anders sein als über \mathbb{Q} : Die elliptische Kurve $E(\mathbb{Q}): y^2 = x^3 + x$ aus Bsp. 3.) V16 etwa enthält den einzigen rationalen Punkt $(0,0)$, über \mathbb{F}_p hat sie aber viele Punkte: Sei $N_p := \#E(\mathbb{F}_p)$ von $y^2 = x^3 + x$, d.h. N_p , die Anzahl der Punkte der elliptischen Kurve $E(\mathbb{F}_p)$, ist die Anzahl der Lösungen von $y^2 = x^3 + x$ modulo p .
- 3.) Numerische Daten ergeben folgende Tabelle:

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	...
N_{p-1}	2	3	3	7	11	19	15	19	23	19	31	35	31	43	47	...

Offenbar gilt $p = N_{p-1}$, falls $p \equiv 3 \pmod{4}$. Für $p \equiv 1 \pmod{4}$ sieht der sogenannte Defekt

$a_p := p+1 - N_p$ aus:

p	5	13	17	29	37	41	53	61	73	89	...
$a_{p/2}$	1	-3	1	5	1	5	-7	5	-3	5	...

Wir halten fest:

Beobachtung: $p - (\frac{a_p}{2})^2$ ist stets Quadratzahl!

- 4.) Für $E(\mathbb{F}_p): y^2 = x^3 + x$ gilt:
- (a) Ist $p \equiv 3 \pmod{4}$, gilt $N_p = p+1$.
- (b) Ist $p \equiv 1 \pmod{4}$, ist $N_p = p+1 \pm 2A$, wobei $p = A^2 + B^2$ mit $2 \nmid A$. Dabei gilt "+" falls $A \equiv 1 \pmod{4}$ und "-" falls $A \equiv 3 \pmod{4}$.

11) Bem.: Fragen über die Größe von N_p führen zu offenen Problemen, z.B. die schwache Vermutung von Birch und Swinnerton-Dyer (1963/65): Für $E(\mathbb{Q})$ mit Koeff. aus \mathbb{Z} sollte

$$\prod_{p \leq x} \frac{N_p}{p} \sim C_E (\log x)^{r(E)}$$

gelten, wobei C_E eine Konstante > 0 ist, die nur von $E(\mathbb{Q})$ abhängig ist.

Die Zahl $r(E)$ ist der Rang von $E(\mathbb{Q})$, vgl. V16. Numerische Untersuchungen stützen diese Vermutung bislang. Sie bedeutet: ist die Anzahl N_p der Punkte auf $E(\mathbb{F}_p)$ bei Reduktion mod p signifikant größer als der Erwartungswert, so sollte der Rang $r(E)$ positiv sein. Sie stellt damit ein numerisch leicht testbares Kriterium für $r(E) > 0$ dar.

Zur Schreibweise \sim : Die Aussage $f(x) \sim g(x)$ für zwei Funktionen $f, g: \mathbb{R}_{>0} \rightarrow \mathbb{R}_{>0}$ bedeutet, dass $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1$, d.h. f, g sind asymptotisch gleich.

12) Weitere numerische Beobachtungen in anderen Beispielen:

Für $E: y^2 = x^3 + 17$ gilt $a_p = 0$ genau für $p \equiv 2 \pmod{3}$,

also auch $a_p = 0$ für "die Hälfte" aller Primzahlen. Das kommt für "wenige" elliptische Kurven mit Koeff. aus \mathbb{Z} so heraus.

Für die Kurve $E: y^2 = x^3 - 4x^2 + 16$ etwa haben wir $a_p = 0$ nur selten:

Die einzigen $p < 2000$ mit $a_p = 0$ sind

$$p = 2, 19, 29, 199, 569, 809, 1289, 1439, \text{ usw.}$$

Welcher der Fälle eintritt, hängt davon ab, ob die elliptische Kurve "komplexe Multiplikation" (Kurz: CM für complex multiplication) hat.

13) Def.: Eine elliptische Kurve $E(\mathbb{R})$ hat komplexe Multiplikation (CM), falls sie neben den üblichen Endomorphismen $\psi_m: E(\mathbb{R}) \rightarrow E(\mathbb{R}), P \mapsto m \cdot P$, wo $m \in \mathbb{Z}$, noch weitere hat.

Elliptische Kurven mit CM haben viele spezielle Eigenschaften, z.B.:

- Elliptische Kurven mit CM haben "ebenso viele" p mit $a_p = 0$ wie p mit $a_p \neq 0$.
- Elliptische Kurven ohne CM haben nur "wenige" p mit $a_p = 0$.

Dennoch konnte N. Elkies 1984 zeigen, dass jede elliptische Kurve $a_p = 0$ für unendlich viele p hat.

- 14.) Beim Übergang von $E(\mathbb{Q})$ mit Koeffizienten $\in \mathbb{Z}$ zu $E(\mathbb{F}_p)$ zu einer Primzahl p reduzieren wir mod p . Nicht immer kommt dabei wieder eine elliptische Kurve heraus, nämlich dann nicht, wenn $\Delta(E(\mathbb{F}_p)) = \underline{0}$ in \mathbb{F}_p gilt, d.h. $p \mid \Delta(E(\mathbb{Q})) \in \mathbb{Z}$.
Wir sprechen dann von schlechter Reduktion, engl.: bad prime,
ansonsten von guter Reduktion, engl.: good prime.

Die schlechte Reduktion kommt nur für alle Primteiler von $\Delta(E(\mathbb{Q})) \in \mathbb{Z}$ vor, also nur für endlich viele Primzahlen p . In diesen Ausnahmefällen verhält sich die kubische Kurve, die durch die Reduktion der Gleichung von $E(\mathbb{Q})$ mod p gegeben ist, oft anders; "+" gibt es dann nicht. Im Bsp. $E(\mathbb{Q}): y^2 = x^3 - 4x^2 + 16$ gilt etwa $N_p \equiv 4 \pmod{5}$ für alle Primzahlen p außer $p=2$ und $p=11$.

Tatsächlich sind $p=2$ und $p=11$ hier die Primzahlen mit schlechter Reduktion, da $\Delta(E(\mathbb{Q})) = -2^{12} \cdot 11$ ist.

- 15.) Für eine elliptische Kurve $E(\mathbb{F}_{p^r})$, $r \geq 1$, wird der Defekt $a_{p^r} = p^r + 1 - N_{p^r}$ auch die "Spur des Frobenius" genannt.
Wir erklären kurz diesen Begriff:

- 16.) Satz & Def.: Der Frobeniusendomorphismus (kurz: Frobenius) einer elliptischen Kurve $E(\mathbb{F}_{p^r})$ ist der durch die Abb. $\phi: \mathbb{P}^2(\overline{\mathbb{F}_{p^r}}) \rightarrow \mathbb{P}^2(\overline{\mathbb{F}_{p^r}})$
 $[x:y:z] \mapsto [x^{p^r}:y^{p^r}:z^{p^r}]$
vermittelte Gruppenhomomorphismus $\Phi: E(\overline{\mathbb{F}_{p^r}}) \rightarrow E(\overline{\mathbb{F}_{p^r}})$.

Beweisskizze: • ϕ ist wirklich eine Abb. von $\mathbb{P}^2(\overline{\mathbb{F}_{p^r}})$ in sich. ✓

• ist $E(\mathbb{F}_{p^r})$ geg. durch $F(x,y,z) = 0$, folgt auch $F(x^{p^r}, y^{p^r}, z^{p^r}) = 0$, weil in $\overline{\mathbb{F}_{p^r}}$ die Gleichung $(c+d)^{p^r} = c^{p^r} + d^{p^r}$ für $c, d \in \overline{\mathbb{F}_{p^r}}$ richtig ist.

Damit ist durch Φ eine Abb. von $E(\overline{\mathbb{F}_{p^r}})$ in sich definiert.

• die Verträglichkeit der Gruppenadd. auf $E(\overline{\mathbb{F}_{p^r}})$ mit Φ , d.h. die Eigenschaft $\Phi(P_1 + P_2) = \Phi(P_1) + \Phi(P_2)$, kann man nachrechnen. □

- 17.) Bem.: Der Frobenius Φ lässt sich auf allgemeinere Strukturen (genau: dem Tate-Modul) übertragen; dieser lässt eine Matrixdarstellung zu, wobei die Spur dieser Matrix genau a_{p^r} ergibt, daher der Name. Dieser Zusammenhang liefert weitere Möglichkeiten, den Defekt a_{p^r} bzw. N_{p^r} zu bestimmen.

18) Text in eine elliptische Kurve einbetten

Bei der Umsetzung des ElGamal-Verschlüsselungsverfahrens für eine elliptische Kurvengruppe $(G, +) = (E(\mathbb{F}_p), +)$, vgl. V6, ist erforderlich, dass sich die kommunizierenden Alice und Bob darauf einigen, wie man Klartext in eine Folge von Punkten auf der elliptischen Kurve $E(\mathbb{F}_p)$ übersetzt und wieder zurück-erhält. Hier ein beispielhaftes Verfahren, wie dies praktisch durchgeführt werden kann:

19) 1. Schritt: Man legt ein Alphabet mit N Buchstaben (identifiziert mit $0, 1, \dots, N-1$) fest. Der Klartext (z.B. ein Wort) habe die Blocklänge l . Die Zuordnung $w = (a_0 a_1 \dots a_{l-1}) \mapsto a_0 N^{l-1} + a_1 N^{l-2} + \dots + a_{l-2} N + a_{l-1} = x_w$ liefert eine Bijektion zwischen den möglichen Klartextblöcken w und den Zahlen $0 \leq x_w < N^l$. Eine Zahl x_w soll x -Koordinate eines Kurvenpunkts werden.

20) 2. Schritt: Für eine geg. elliptische Kurve $E(\mathbb{F}_p)$ gibt es aber nicht zu jedem $x_0 \in \mathbb{F}_p$ einen Kurvenpunkt $(x_0, y_0) \in E(\mathbb{F}_p)$. Für ein $k \in \mathbb{N}$ kann man aber die nächste x -Koordinate eines Kurvenpunkts $(x_1, y_1) \in E(\mathbb{F}_p)$ mit $x_0 \leq x_1 < x_0 + k$ schnell ermitteln; die Wahrscheinlichkeit, dass dies scheitert, d.h. dass ein solches x_1 nicht ex., beträgt schätzungsweise nur $\approx (\frac{1}{2})^k$. (Bsp.: $k=50 \rightsquigarrow (\frac{1}{2})^{50} < 10^{-15}$) Wähle so ein geeignetes k fest und eine elliptische Kurve $E(\mathbb{F}_p)$ mit $p > k \cdot N^l$, d.h. es gibt wohl Kurvenpunkte mit genügend großen x -Koordinaten.

21) 3. Schritt: Zu $x_w \in \{0, \dots, N^l - 1\}$ bestimme $P_w \in E(\mathbb{F}_p)$ mit x -Koordinate $\geq kx_w$, etwa $P_w = (kx_w + j, y)$ mit $j \geq 0$ minimal.

22) Beobachtung: Hat das Verfahren funktioniert, ist dabei $j < k$, so dass durch Berechnung von $x_w = \lfloor \frac{x}{k} \rfloor$ für $P_w = (x, y) \in E(\mathbb{F}_p)$ der Plaintext w aus P_w wieder zurückgewonnen werden kann.

23) Bsp.: Für das Alphabet $\{A, B, \dots, Z\} = \{0, 1, \dots, 25\}$ ist $N=26$, wähle z.B. $l=2, k=10$. Dann erfüllt $p=6833$ die Bedingung $p > kN^2 = 6760$. Ist dazu $E(\mathbb{F}_p)$ geg. durch $E(\mathbb{F}_p): y^2 = x^3 + 5984x + 1180$, kann z.B. der Text "KRYPTO" wie folgt in eine Liste von 3 Punkten auf $E(\mathbb{F}_p)$ umgesetzt werden:

w	KR	YP	TO
x_w	$(10, 17)_{26} = 277$	$(24, 15)_{26} = 639$	$(19, 14)_{26} = 508$
P_w	$(2771, 353)$	$(6390, 2797)$	$(5080, 238)$